EXHIBIT A

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1625 Dyre Street, Apartment D
Philadelphia, Pennsylvania 19124

Case No. 18-1446-M

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before September 26, 2018 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any Magistrate Judge in the EDPA.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: 9/13/18 10:25 AM

Judge's signature

City and state: Philadelphia, Pennsylvania

Marilyn Heffley, United States Magistrate Judge
Printed name and title

000021

EXHIBIT A

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 18 -_____-M	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

EXHIBIT A

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1625 Dyre Street, Apartment D
Philadelphia, Pennsylvania 19124

Case No. 18 - 1446 -M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252	Illegal distribution, transportation, receipt, and possession of child pornography

The application is based on these facts:
See attached affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days ~~(give exact ending date if more than 30 days: _____)~~ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Rebecca Quinn
Applicant's signature

Rebecca Quinn, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/12/2018

Marilyn Heffley
Judge's signature

City and state: Philadelphia, Pennsylvania

Marilyn Heffley, U.S. Magistrate Judge
Printed name and title

EXHIBIT A

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Rebecca A. Quinn, being duly sworn and state as follows:

INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation (FB, United States Department of Justice. I have been employed as a Special Agent of the FBI since April 2002. I am currently assigned to the Philadelphia Division, Crimes Against Children squad, working primarily on cases involving online crimes against children, where I have become familiar with the methods and schemes employed by persons who trade and collect child pornography. As a federal agent, I am authorized to investigate violations of laws of the United States and am a "federal law enforcement officer" within the meaning of Fed. R. Crim. P. 41(a)(2)(C). I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2252. I have also participated in various FBI-mandated and other training for the investigation and enforcement of federal statutes prohibiting the production, distribution, and possession of child pornography.

2. This affidavit is being made in support of an application for a search warrant authorizing the search of 5924 Tackawanna Street, Philadelphia, Pennsylvania 19135, which has been pictured and more fully described in Attachment A; and 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124, which has been pictured and more fully described in Attachment A-1 of this affidavit, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1), 2252(a)(2), and 2252(a)(4)(B), which items are more specifically described in Attachment B of this Affidavit.

3. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(1), 2252(a)(2), and 2252(a)(4)(B), have been committed, and that evidence of those violations are presently located at 5924 Tackawanna Street, Philadelphia, Pennsylvania 19134, and 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124.

APPLICABLE STATUTES

4. 18 U.S.C. § 2252(a)(1) and (b)(1) make it a crime to knowingly ttransport, or attempt or conspire to transport, using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means including by computer, a visual depiction of a minor engaged in sexually explicit conduct, produced using a minor engaged in such conduct.

5. 18 U.S.C. § 2252(a)(2) and (b)(1) make it a crime to knowingly receive or distribute, or attempt or conspire to receive or distribute, any visual depiction, using any means or facility of interstate or foreign commerce or which has been mailed, or that has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been so shipped or transported, by any means including by computer, a visual depiction of a minor engaged in sexually explicit conduct, produced using a minor engaged in such conduct.

6. 18 U.S.C. § 2252(a)(4)(B) makes it a crime to knowingly possess one or more matters which contain any visual depiction of a minor engaged in sexually explicit conduct, produced using a minor engaged in such conduct, that has been mailed or that has been transported

using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or were produced using materials that were mailed or so transported, by any means including by computer.

7. "Sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) as actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or the lascivious exhibition of the genitals or pubic area of any person.

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. A "Hash Value" is a mathematical value generated by applying an algorithm to a computer file that is represented by a sequence of hexadecimal digits. Among computer forensics professionals, a hash value is generally considered to be a unique signature or fingerprint for a file.

f. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

k. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

l. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

9. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload

that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

10. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who collect child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material,

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, in this case, even if the suspect target uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in both residences, 5924 Tackawanna Street, Philadelphia, Pennsylvania 19135 and 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124, as set forth in Attachment A and A-1.

11. Based on the information set forth below, I submit there is probable cause to believe that subject target NATHAN WEYERMAN is a collector of child pornography, based in part on the fact that he installed Freenet software and requested a higher number of blocks associated with child exploitation files.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

12. The instant investigation involves a user of "Freenet" — which is an Internet-based, peer-to-peer (P2P) network that allows users to anonymously share files, chat on message boards, and access websites within the network. Law enforcement agents have been investigating child pornography trafficking by Freenet users since at least 2011.

A. Background Regarding Freenet

13. In order to access Freenet, a user must first download the Freenet software, which is free and publicly available. The Freenet "source code" — i.e., the computer programming code that facilitates Freenet's operation – is also publicly available. In other words, Freenet is

"open source" software that may be examined and analyzed by anyone with the pertinent expertise or knowledge.

14. Anyone running the Freenet software may join and access the Freenet network. Each computer running Freenet connects directly to other computers running Freenet, which are called its "peers."[2] When installing Freenet, each user agrees to provide to the network a portion of the storage space on the user's computer hard drive, so that files uploaded by Freenet users can be distributed and stored across the network. Freenet users can upload files into the Freenet network and download files from the Freenet network. After a user installs Freenet on the user's computer, the software creates a default "download" folder. If a user successfully downloads a particular file from Freenet, Freenet may save the content of that file to the "download" folder. A user may change this default setting and direct the content to be downloaded elsewhere.

15. When a user uploads a file into Freenet, the software breaks the file into pieces (called "blocks") and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Freenet network of peers.[3] The software also creates an index piece that contains a list of all of the pieces of the file and a unique key – a series of letters, numbers and special characters – that is used to download the file.[4]

---

[2] The number of peers is determined by the user's settings and is based on the quality and speed of the user's Internet connection.

[3] Because the pieces of files are encrypted, a Freenet user is unable to access the content of pieces that are stored on the user's computer hard drive, which are not in a readable format.

[4] An example key is: CHK@0R6h6o8a~JbOGg8GmxGauRyqJPSwcHGmxGauLznw8Fey B0go,08agxRpNx~wc~rmZRfWQaSed3HTeKKkXAwvDRF2LUaU,AAMC--8/lolitaz49.avi.

EXHIBIT A

16. In order to download a file on Freenet, a user must have the key for the file. There are a number of ways that a Freenet user can download a file using a key. Some examples include: (1) the "download" box on Freenet's "file sharing" page; (2) the "download" box on the message board associated with Freenet or other Freenet add-on programs; and (3) directly through the user's web browser while the user is connected to the Freenet network.

17. When a user attempts to download a file via Freenet, Freenet downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Freenet software then requests all of the pieces of the file from the user's peers. Rather than request all of the file pieces from a single peer, requests for file pieces are divided up in roughly equal amounts among the user's peers. If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on. For example, if User "A" has 10 peers and requests 1000 pieces of a file, roughly 100 pieces are requested from each one of User A's peers. See Figure 1.

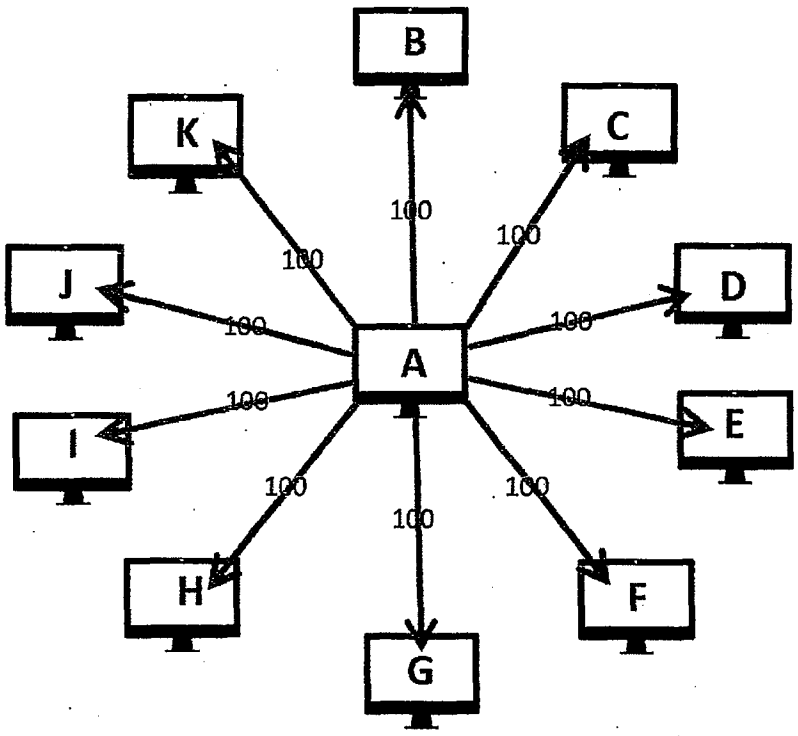

Figure 1

If Peer "B" receives User A's request for 100 pieces of the file, but does not have any of those pieces in its storage, Peer B forwards on the request for those pieces to Peer B's peers. If Peer B has 10 peers of its own, roughly 10 pieces are requested from each one of Peer B's peers. See Figure 2.

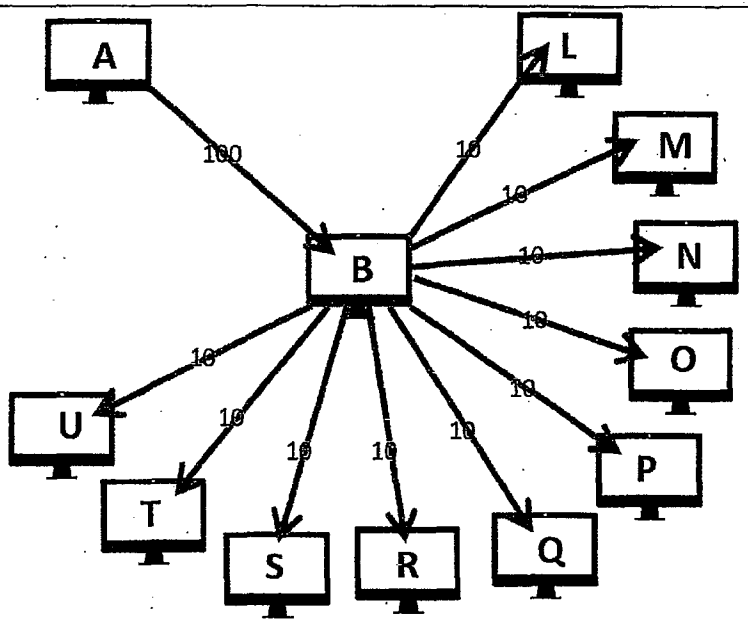

Figure 2

As noted below, this design can help law enforcement distinguish between a Freenet user that is the original requestor of a file, and one that is merely forwarding the request of another user.

18. To prevent requests for pieces from going on indefinitely, Freenet is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times (the default maximum is 18). The remaining number of times a request for a piece may be forwarded is included within the request for that piece. If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers.

19. Freenet attempts to hide which computer uploaded a file into or downloaded a file from the network by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer (i.e., the peer was the "original requestor" of the file), or whether that peer was simply forwarding a different peer's request. Freenet attempts to

hide the identity of the original requestor by randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor of the file. This design allows investigators using Freenet to focus investigative efforts on peer computers that request pieces of files of interest that may be forwarded 17 or 18 times, in order to determine whether the peer was the original requestor of the file.

20. Freenet has two operational modes, "Darknet" and "Opennet." On the Darknet mode, a computer connects only to peers whom the user has specifically selected. On the Opennet mode, a computer may connect to peers unknown to the user. A Freenet user may choose which mode to use. The mode relevant to this investigation involves a user who chose to use the Opennet operational mode.

21. Freenet warns its users in multiple ways that it does not guarantee anonymity: when Freenet software is initially installed; within the log file each time Freenet is started; and via Freenet's publicly accessible website. Freenet software also does not mask a computer's IP address — the IP addresses of each Freenet user's peers are observable to the user. For example, if a user is connected to 10 peers on Freenet, all 10 of those peers' IP addresses will be observable to the user. The fact that Freenet does not mask IP addresses is explained on its publicly accessible website. Freenet also acknowledges on its publicly accessible website that, for users who use the Opennet mode, it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

B. Child Pornography Images/Videos on "Freenet"

22. Freenet can be used to advertise, distribute, and receive images and videos of child pornography. Unlike other file sharing systems, Freenet does not provide a search function for its users whereby users would insert search terms to locate files. Therefore, a user who wishes to locate and download child pornography from Freenet must identify the key associated with a particular child pornography file and then use that key to download the file.

23. Freenet users can identify those keys in a number of ways. For example, "message boards" exist on Freenet that allow users to post textual messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: "pthc," "boy porn," "hussy," "pedomom," "kidfetish," "toddler_cp," "hurtcore," and "tor-childporn." Typical posts to those message boards contain text, keys of child pornography files that can be downloaded through Freenet, and in some cases descriptions of the image or video file associated with those keys.

24. Freenet users can also obtain keys of child pornography images or videos from websites that operate within Freenet called "Freesites." Freesites can only be accessed through Freenet. Some of those sites contain images of child pornography the user can view along with keys of child pornography files. It is also possible that Freenet users may obtain keys related to child pornography images or videos directly from other Freenet users.

C. Investigation into the Trafficking of Child Pornography on Freenet

25. Since approximately 2011, law enforcement has been investigating the trafficking of child pornography on Freenet. A modified version of the Freenet software is available to sworn law enforcement officers to assist in conducting Freenet investigations. This law enforcement version is nearly identical to Freenet, except that it allows a computer operated

by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers. The types of information logged by a law enforcement computer are available to all standard Freenet users as part of Freenet's normal operation. This information includes, but is not limited to: the IP addresses of the user's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Freenet "location"); the remaining number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.

26. Law enforcement computers do not target specific peers on Freenet nor do law enforcement computers solicit requests from any peers. The Freenet information collected by law enforcement computers is logged and provided to other Freenet-trained law enforcement personnel in order to further investigations into Freenet users believed to be downloading child pornography files through Freenet.

27. Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on Freenet. Law enforcement only investigates Freenet users who request pieces of files associated with such keys collected by law enforcement. The keys collected by law enforcement have been obtained via publicly accessible sites, such as Freenet message boards and Freesites, as well as during the course of prior investigations into child pornography trafficking on Freenet. This investigation pertains to child pornography files with known keys, the content of which are further described below. Those files are referenced as "files of interest."

28. By viewing the documented activity of a peer that sends a request to a law enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of a file of interest. Only those requests that were intended

for law enforcement computers as recipients, that are forwarded 17 or 18 times, and are associated with a file of interest are analyzed. A mathematical formula is then applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer.

29. Your affiant has reviewed a peer-reviewed, publicly-available academic paper describing the methodology of that mathematical formula. In basic terms, the methodology relies on two primary facts about the Freenet software: first, the original requestor divides up its requests for pieces of a file among its peers, sending a roughly equal fraction of the requests to each peer; second, if a peer does not have the requested pieces, the peer takes the fraction of requests for pieces of a particular file and divides them up again among its own peers. See Figures 1 and 2. Because a peer that is merely routing another peer's request would ask its peers for a significantly smaller portion of the pieces of a file than an original requester, it is possible for the recipient of requests to determine whether a request is significantly more likely than not from an original requestor. The academic paper's detailed evaluation finds that a formal mathematical formula based on this reasoning is highly accurate (specifically, it has a high true positive rate and a low false positive rate). Based upon my training and experience, I believe this to be a reliable method to determine whether it is significantly more probable than not that that a given Freenet computer is the original requestor of a file of interest.

30. I am also aware through my training and experience that dozens of searches of digital devices have been conducted by law enforcement officers (either through court-authorization or consent) related to targets whose IP addresses were identified based upon analysis of information from Freenet law enforcement computers, pursuant to which evidence of child pornography possession and/or trafficking was located.

D. Requests Targeted in the Instant Investigation

31. I have reviewed information obtained and logged by law enforcement Freenet computers related to IP address 100.11.199.85. Such information shows that a Freenet user with IP address 100.11.199.85 requested pieces of the child pornography files described below from a law enforcement Freenet computer. With respect to each file – considering the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had – the number of requests for file pieces is significantly more than one would expect to see if the user of IP address 100.11.199.85 were merely routing the request of another user. Accordingly – based on my review of those records, my understanding of Freenet, my training and experience, and the fact that the same user requested pieces of multiple child pornography files – I believe that the user of IP 100.11.199.85 was the original requestor of each of the files described below.

32. On September 18, 2017 between 4:42 am and 6:13 am UTC, a computer running Freenet software, with an IP address of 100.11.199.85, requested from Freenet law enforcement nodes, 71 unique blocks of the file name, "pthc webcam 2012 natalia zuleta 02.avi" with a SHA1 digital hash value of SB6FHDWFK3QKMK6JWIFJFFNWLDGBUTL6[5]. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet and know it to be a video of a minor female exposing her vagina and masturbating.

33. On September 18, 2017 between 4:45 am and 6:42 am UTC, a computer running Freenet software, with an IP address of 100.11.199.85, requested from Freenet law

[5] "SHA1" stands for "secure hash algorithm – 1" and refers to a particular type of cryptographic hash value.

enforcement nodes, 107 unique blocks of the file name, "Jessica and lexi epic lez.avi" with a SHA1 digital hash value of H6J7LRZCAL4VGHQIMNCJUPO5PLIUVRPF. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet and know it to be a video of a nude, minor female, masturbating. Another nude, minor female joins in the video and they masturbate each other.

34. On October 19, 2017 between 11:42 pm and October 20, 2017 at 12:18 am UTC, a computer running Freenet software with an IP address 100.11.199.85, requested from Freenet law enforcement nodes, 66 unique blocks of the file name, "pzm01-02-05.avi" with SHA1 digital hash value of IOSASH5UQYTT2KT4S6C3NB73YUA3IS7A. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet and know it to be a video of a nude, minor female in the bathtub, who gets out, dries off and puts her clothes on.

35. On February 1, 2018 between 3:48 pm and 3:58 pm UTC, a computer running Freenet software with an IP address 100.11.199.85, requested from Freenet law enforcement nodes, 21 unique blocks of the file name, "1-josiealeyna03.flv" with SHA1 digital hash value of QSU5X2BHPLAPRAXMCXWEBY3WFO3UHYOY. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet and know it to be a video of a prepubescent girl, not wearing underwear and masturbating.

36. The fact that a Freenet user requested pieces associated with a particular file on Freenet indicates that the user attempted to download the file's contents from Freenet. It does not indicate whether or not the user successfully retrieved all of the necessary pieces to successfully download the file.

IDENTIFICATION OF THE SUBJECT PREMISES

37. Using publicly available search tools, law enforcement determined that IP address 100.11.199.85 was controlled by Verizon Internet Service Provider ("ISP").

38. On or about January 9, 2018 an administrative subpoena was provided to Verizon for subscriber information relating to the use of IP address 100.11.199.85. A review of the results obtained revealed the following account holder and address: NATHAN WEYERMAN, 5924 Tackawanna Street, Philadelphia, Pennsylvania 19135.

39. A check of publicly available databases also revealed that NATHAN WEYERMAN resides at 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124.

40. An administrative subpoena was sent to Verizon Internet, who confirmed that there is internet service at 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124, and the subscriber is NATHAN WEYERMAN.

41. WEYERMAN is a Tier I Megan's Law sex offender. In September 2005, he pleaded guilty to rape (18 Pa.C.S. § 3121), involuntary deviate sexual intercourse with complainant who is less than 13 years of age (18 Pa.C.S. § 3123), and corruption of minors (18 Pa.C.S. § 6301). As part of his sentence on these convictions, WEYERMAN is currently being supervised by Philadelphia County Probation and Parole.

42. On June 14, 2018, WEYERMAN's Philadelphia County Probation Officer, Francis Dragon confirmed that WEYERMAN's residence is 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124. PO Dragon also advised that at times WEYERMAN also stays with his girlfriend at her residence, 5924 Tackawanna Street,

Philadelphia, Pennsylvania 19135, but his address of record with the State Probation Office remains the Dyre Street apartment.

43. On June 14, 2018, United States Postal Inspection Services confirmed WEYERMAN receives mail at both residences: 5924 Tackawanna Street, Philadelphia, Pennsylvania 19135 and at 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124. As noted above in paragraphs 38 and 40, the internet service at both residences is in WEYERMAN's name as well.

44. On September 4, 2018, Probation Officer Dragon visited WEYERMAN at 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124. Officer Dragon completed a standard walk through of the residence and did not notice any computer media in plain sight. Officer Dragon stated if any media was viewable in plain sight it would be subject to search.

45. A check of the Pennsylvania Megan's Law website on September 12, 2018 confirmed that WEYERMAN last registered his address with the Pennsylvania State Police on April 3, 2018, and listed it as 1625 Dyre Street, Apartment D, Philadelphia, PA 19124.

46. Based upon your Affiant's training and experience, your Affiant knows that some users who distribute, transport, receive, and possess child pornography transfer these files between their different electronic devices and online accounts, whether it is to conceal the files or store them in one device or account versus another device or account. In addition, as stated above in paragraph 10(g), it is common for collectors of child pornography to keep their collections or portions of their collections with them, stored electronically on various electronic devices. For these reasons, and those outlined in this affidavit, there is probable cause to believe

that evidence of child pornography will be found at both the Tacawanna Street and Dyre Street residences.

ABILITY TO RETRIEVE DELETED FILES

47. Computer files or remnants of such files on traditional or conventional mechanical computer hard drives can typically be recovered months or even years after they have been downloaded onto the hard drive, deleted or viewed via the Internet. Electronic files downloaded to the hard drive or storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from these conventional types of hard drives depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

48. Other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory based hard drives and devices. This

technology has been traditionally used for small thumb drives where files and data are stored electronically, but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and overwritten. Because of how these flash, memory-based drives function it may limit how much data, if any, can be recovered from these types of devices.

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at both residences, 5924 Tackawanna Street, Philadelphia, Pennsylvania 19135 described in Attachment A1 and 1625 Dyre Street, Apartment D, Philadelphia, Pennsylvania 19124 described in Attachment A2. I respectfully request that this Court issue a search warrant for the locations described in Attachments A1 and A2, authorizing the seizure and search of the items described in Attachment B.

50. I further respectfully submit that public disclosure of the existence of this search warrant affidavit and its accompanying materials at this juncture could jeopardize the

government's ongoing investigation in this case, and therefore respectfully request that this affidavit and all accompanying material be sealed until further order of this Court.

Respectfully submitted,

Rebecca A. Quinn
Special Agent, Federal Bureau of Investigation

Sworn and subscribed
Before me this 13th
day of September 2018.

HONORABLE MARILYN HEFFLEY
United States Magistrate Judge